IN THE CLAIMS

Please amend the claims as indicated:

1. (currently amended) A method for managing a secure network boot of a server blade, the server blade being in a blade chassis that has multiple server blades, the blade chassis including a switching means allowing the server blade to communicate with a network, the method comprising:

storing a list of trusted management servers in a management module on a server blade;

broadcasting a Dynamic Host Configuration Protocol (DHCP) DISCOVER request to a network of DHCP servers;

~~broadcasting a request for a boot program from a server blade to a network of management servers;~~

receiving, at a switching means associated with the server blade, a DHCP OFFER message that is responsive to the DHCP DISCOVER request, wherein the DHCP OFFER message contains Internet Protocol (IP) addresses of responding DHCP servers, a Dynamic IP address with lease information, and a list of Pre-boot eXecution Environment (PXE) Boot Servers that can be contacted by the server blade to download a boot program, and wherein the DHCP OFFER comes from a responding DHCP server on the network of DHCP servers;

~~receiving a response to the request for the boot program at a switching means associated with the server blade, the response being from a responding management server on the network of management servers, the response containing directions to a boot program server;~~

comparing an identity of the responding [[management]] DHCP server with the list of trusted [[management]] DHCP servers in the management module on the server blade; and

[[upon]] in response to verifying that the responding [[management]] DHCP server is on the list of trusted [[management]] DHCP servers, ~~transmitting the response from the responding management server to the server blade~~ permitting the DHCP OFFER message to pass through to the server blade via an Ethernet switch that is coupled to the server blade, and downloading a boot program from a boot program server specified by the responding [[management]] DHCP server.

2. (currently amended) The method of claim 1, further comprising:

[[upon]] in response to determining that the responding [[management]] DHCP server is not on the list of trusted [[management]] DHCP servers, blocking the transmittal of the response from the responding [[management]] DHCP server through the Ethernet switch to the server blade.

3. (currently amended) The method of claim 2, further comprising:

[[upon]] in response to determining that the responding [[management]] DHCP server is not on the list of trusted [[management]] DHCP servers, generating an alert to a designated administrator server of a presence of an unauthorized [[management]] DHCP server on the network of [[management]] DHCP servers.

4. (cancelled)

5. (currently amended) The method of claim [[4]] 1, ~~wherein the comparing step is performed by configuring the Ethernet switch to perform Layer 3 packet filtering to identify Pre-boot Execution Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the seven layers of the Open System Interconnection (OSI) model~~ wherein none of the steps described in claim 1 causes any code changes to firmware in the server blade.

6. (original) The method of claim 1, further comprising:

upon determining that the responding management server is not on the list of trusted management servers, downloading a boot program from a known trusted boot server in a secure local area network (LAN).

7. (original) The method of claim 1, further comprising:

managing different types of boot program servers available to the server blade by maintaining, in an information technology services organization logically oriented between the different types of boot program servers and the server blade, a permission list of boot program servers authorized for each server blade in a server blade chassis.

8. (currently amended) A system for managing a secure network boot of a server blade, the server blade being in a blade chassis that has multiple server blades, the blade chassis including a switching means allowing the server blade to communicate with a network, the system comprising:

means for storing a list of trusted management servers in a management module on a server blade;

means for broadcasting a Dynamic Host Configuration Protocol (DHCP) DISCOVER request to a network of DHCP servers;

~~means for broadcasting a request for a boot program from a server blade to a network of management servers;~~

means for receiving, at a switching means associated with the server blade, a DHCP OFFER message that is responsive to the DHCP DISCOVER request, wherein the DHCP OFFER message contains Internet Protocol (IP) addresses of responding DHCP servers, a Dynamic IP address with lease information, and a list of Pre-boot eXecution Environment (PXE) Boot Servers that can be contacted by the server blade to download a boot program, and wherein the DHCP OFFER comes from a responding DHCP server on the network of DHCP servers;

~~means for receiving a response to the request for the boot program at a switching means associated with the server blade, the response being from a responding management server on the network of management servers, the response containing directions to a boot program server;~~

means for comparing an identity of the responding [[management]] DHCP server with the list of trusted [[management]] DHCP servers in the management module on the server blade; and

means for, [[upon]] in response to verifying that the responding [[management]] DHCP server is on the list of trusted [[management]] DHCP servers, ~~transmitting the response from the responding management server to the server blade~~ permitting the DHCP OFFER message to pass through to the server blade via an Ethernet switch that is coupled to the server blade, and downloading a boot program from a boot program server specified by the responding [[management]] DHCP server.

9. (currently amended) The system of claim 8, further comprising:

means for, [[upon]] in response to determining that the responding [[management]] DHCP server is not on the list of trusted [[management]] DHCP servers, blocking the transmittal of the response from the responding [[management]] DHCP server through the Ethernet switch to the server blade.

10. (currently amended) The system of claim 9, further comprising:

means for, [[upon]] in response to determining that the responding [[management]] DHCP server is not on the list of trusted [[management]] DHCP servers, generating an alert to a designated administrator server of a presence of an unauthorized [[management]] DHCP server on the network of [[management]] DHCP servers.

11. (cancelled)

12. (currently amended) The system of claim [[11]] 9, ~~wherein the means for comparing configures the Ethernet switch to perform Layer 3 packet filtering to identify Pre-boot Execution Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the seven layers of the Open System Interconnection (OSI) model~~ wherein none of the steps described in claim 1 causes any code changes to firmware in the server blade.

13. (original) The system of claim 8, further comprising: means for, upon determining that the responding management server is not on the list of trusted management servers, downloading a boot program from a known trusted boot server in a secure local area network (LAN).

14. (original) The system of claim 8, further comprising:

means for managing different types of boot program servers available to the server blade by maintaining, in an information technology services organization logically oriented between the different types of boot program servers and the server blade, a permission list of boot program servers authorized for each server blade in a server blade chassis.

15. (currently amended) A computer program product, residing on a computer usable medium, for managing a secure network boot of a server blade, the server blade being in a blade

chassis that has multiple server blades, the blade chassis including a switching means allowing the server blade to communicate with a network, the computer program product comprising:

program code for storing a list of trusted management servers in a management module on a server blade;

program code for broadcasting a Dynamic Host Configuration Protocol (DHCP) DISCOVER request to a network of DHCP servers;

~~program code for broadcasting a request for a boot program from a server blade to a network of management servers;~~

program code for receiving, at a switching means associated with the server blade, a DHCP OFFER message that is responsive to the DHCP DISCOVER request, wherein the DHCP OFFER message contains Internet Protocol (IP) addresses of responding DHCP servers, a Dynamic IP address with lease information, and a list of Pre-boot eXecution Environment (PXE) Boot Servers that can be contacted by the server blade to download a boot program, and wherein the DHCP OFFER comes from a responding DHCP server on the network of DHCP servers;

~~program code for receiving a response to the request for the boot program at a switching means associated with the server blade, the response being from a responding management server on the network of management servers, the response containing directions to a boot program server;~~

program code for comparing an identity of the responding [[management]] DHCP server with the list of trusted [[management]] DHCP servers in the management module on the server blade; and

program code for, [[upon]] in response to verifying that the responding [[management]] DHCP server is on the list of trusted [[management]] DHCP servers, ~~transmitting the response from the responding management server to the server blade~~ permitting the DHCP OFFER message to pass through to the server blade via an Ethernet switch that is coupled to the server blade, and downloading a boot program from a boot program server specified by the responding [[management]] DHCP server.

16. (currently amended) The computer program product of claim 15, further comprising:

program code for [[upon]] in response to determining that the responding [[management]] DHCP server is not on the list of trusted [[management]] DHCP servers, blocking the transmittal of the response from the responding [[management]] DHCP server through the Ethernet switch to the server blade.

17. (currently amended) The computer program product of claim 16, further comprising:

program code for, [[upon]] in response to determining that the responding [[management]] DHCP server is not on the list of trusted [[management]] DHCP servers, generating an alert to a designated administrator server of a presence of an unauthorized [[management]] DHCP server on the network of [[management]] DHCP servers.

18. (cancelled)

19. (currently amended) The computer program product of claim [[18]] 15, ~~wherein the comparing step is performed by configuring the Ethernet switch to perform Layer-3 packet filtering to identify Pre boot Execution Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the seven layers of the Open System Interconnection (OSI) model~~ wherein none of the steps described in claim 1 causes any code changes to firmware in the server blade.

20. (original) The computer program product of claim 15, further comprising:

program code for, upon determining that the responding management server is not on the list of trusted management servers, downloading a boot program from a known trusted boot server in a secure local area network (LAN).

21. (original) The computer program product of claim 15, further comprising:

program code for coordinating different types of boot program servers available to the server blade by maintaining, in an information technology services organization logically oriented between the different types of boot program servers and the server blade, a permission list of boot program servers authorized for each server blade in a server blade chassis.

22. (new) The method of claim 7, wherein the information technology services organization is an Information Technology (IT) services organization that manages various types of Pre-boot

eXecution Environment (PXE) deployment servers, and wherein the IT services organization enables a same IT service organization assigned systems administrator to manage the various types of PXE deployment servers, to maintain permission lists for each PXE server type, to monitor a network for a presence of unauthorized PXE servers that are not authorized, by the IT services organization, to support the client computer, and to shut down network ports, for unauthorized PXE servers, in the client computer.

23. (new) The system of Claim 14, wherein the information technology services organization is an Information Technology (IT) services organization that manages various types of Pre-boot eXecution Environment (PXE) deployment servers, and wherein the IT services organization enables a same IT service organization assigned systems administrator to manage the various types of PXE deployment servers, to maintain permission lists for each PXE server type, to monitor a network for a presence of unauthorized PXE servers that are not authorized, by the IT services organization, to support the client computer, and to shut down network ports, for unauthorized PXE servers, in the client computer.

24. (new) The computer program product of Claim 21, wherein the information technology services organization is an Information Technology (IT) services organization that manages various types of Pre-boot eXecution Environment (PXE) deployment servers, and wherein the IT services organization enables a same IT service organization assigned systems administrator to manage the various types of PXE deployment servers, to maintain permission lists for each PXE server type, to monitor a network for a presence of unauthorized PXE servers that are not authorized, by the IT services organization, to support the client computer, and to shut down network ports, for unauthorized PXE servers, in the client computer.